

RIVEST-SHAMIR-ADLEMAN PUBLIC KEY CRYPTOSYSTEMS DO NOT ALWAYS CONCEAL MESSAGES

G. R. BLAKLEY and I. BOROSH†

Department of Mathematics, Texas A & M University, College Station, TX 77843, U.S.A.

Communicated by E. Y. Rodin

(Received July 1978, and in revised form October 1978)

Abstract—To every pair p, q of distinct primes there correspond 9 positive integers x no larger than pq such that

$$x^c = x \pmod{pq}$$

for every odd positive integer c . Therefore these 9 messages x are unconcealable in any Rivest-Shamir-Adleman public key cryptosystem which has the product pq for its encoding modulus. There are, in fact, such cryptosystems which do not conceal any messages, and others which conceal less than 50% of all messages possible within them. These examples point up the need for effective criteria for evaluating the concealing power of any such cryptosystem. This paper treats these questions for a general square free encoding modulus m . It contains easy to use necessary and sufficient conditions that the function $f(x) = x^c$ be:

1. a permutation of the residue classes modulo m ;
2. a derangement (i.e. a permutation without fixed points) of the collection of all the residue classes modulo m other than the unavoidably unconcealable ones.

It also provides a construction of all such "deranging" exponents.

1. INTRODUCTION

Until a few years ago codes and ciphers in common use suffered from a serious drawback. If you gave somebody a key which allowed him to use a piece of cryptographic equipment to encode a message you also, by that very act, gave him the wherewithal to decode (i.e. take the transmitted ciphertext message and recover the original cleartext message which gave rise to it) every message which has been encoded on that equipment with that key.

Diffe and Hellman recently pointed out that this need not always be the case. In fact an English to Spanish dictionary (the encoding key) helps you to "encode" a message written in English by translating it into Spanish, but does not help you to "decode" the message by translating the Spanish text back to English. For that you need a Spanish to English dictionary (the separate decoding key).

Suppose there is a way to produce a cleartextish to ciphertextish dictionary with so many entries and so seemingly confusing a structure that nobody but you (who know the method behind the ostensible madness of its construction) can sort it so as to produce a ciphertextish to cleartextish dictionary. Then you can give copies of the former dictionary (the public encoding key) to everybody in the world and keep your one copy of the latter dictionary (your private decoding key). In this case you have established a public key cryptosystem enabling everybody to encode messages for sending to you.

Rivest *et al.* [4] did this, and a bit more. It is routine to turn written, spoken, and even pictorial messages into lists of bit strings. So they defined a message to be a positive integer x smaller than 10^{200} . Both cleartext messages and ciphertext messages are of this form. They then asked any potential message receiver R to find two primes p and q larger than 10^{100} and two integers c and d between 3 and $m = pq$ such that $cd \equiv 1 \pmod{(p-1)(q-1)}$. They asked the receiver R to keep p, q and d secret, but to announce c and m to the world. Anybody wishing to form the encoded message y corresponding to a cleartext message x finds the smallest positive integer y such that $y \equiv x^c \pmod{m}$. This is how the sender constructs the cleartextish to ciphertextish half of the dictionary. When receiver R gets the message y he forms the smallest positive integer z such that $z \equiv y^d \pmod{m}$. This is how the receiver constructs the ciphertextish to cleartextish half of the

†This author was partially supported by NSF grant MCS76-06092.

dictionary. It follows from a short argument based on Fermat's theorem and the way c and d were chosen above that $z \equiv (x^c)^d \equiv x^1 \pmod{m}$ and, consequently, that $z = x$. The idea is that it is hard to factor numbers as large as m but it is easy to find primes as big as p and q . So the fact that only the receiver R knows the factorization of m seems to entail that only the receiver R knows how to decode messages.

The article [4] aforementioned has more background and shows how to give unforgeable signatures by telegraph or telex, an important feature not shared by many other cryptosystems, even many other public key cryptosystems. In this paper we will modify the procedure described above and in [4] to avoid a possibly unfortunate choice of coding exponent c . To see what can happen if the message receiver R does not take additional precautions consider the following example.

Suppose that

$$\begin{aligned} p &= 97 \\ q &= 109 \\ m &= 10573 \\ c &= 865 \\ d &= 9505. \end{aligned}$$

Then obviously

$$\begin{aligned} m &= 97 * 109 = pq \\ \phi(p) &= p - 1 = 96 \\ \phi(q) &= q - 1 = 108 \\ \phi(m) &= (p - 1)(q - 1) = 96 * 108 = 10368 \\ cd &= 8221825 = 1 + 793 * 10368. \end{aligned}$$

Consequently

$$cd \equiv 1 \pmod{(p - 1)(q - 1)}.$$

From all these facts it is immediate that there is a Rivest-Shamir-Adleman (RSA) public key cryptosystem [4] which has:

$$\begin{aligned} 10573 &= m \text{ as its public encoding modulus;} \\ 865 &= c \text{ as its public encoding exponent;} \\ 9505 &= d \text{ as its private decoding exponent.} \end{aligned}$$

But this cryptosystem provides no concealment. The encoded form of every single message is exactly the same as the cleartext. In other words

$$x^{865} \equiv x \pmod{10573}$$

for every integer x . This can be verified numerically. But it also follows readily from [1] or [3, 1-80]. If we change only c and d above, so that

$$\begin{aligned} c &= 169 \\ d &= 3865 \\ cd &= 653185 = 1 + 63 * 10368 \end{aligned}$$

then it is not hard to verify that there are 325 unconcealed messages out of 10573. This latter cryptosystem has a concealment rate between 96% and 97%, compared to 0% for the cryptosystem which used

$$c = 865$$

for its coding exponent.

The foregoing statements are all easy to verify on the basis of the development below. But we ask the reader to accept them at face value for the moment. These examples were adduced, not as isolated peculiarities, but to motivate the threefold purpose of this paper, which is to provide:

1. A proof that the Rivest-Shamir-Adleman sufficient condition on c and m that the function

$$f(x) = x^c$$

effect a permutation of the residue classes modulo m is also a necessary condition;

2. A uniform lower bound, independent of the public encoding modulus m and the public encoding exponent c , to the number of unconcealable messages in a Rivest-Shamir-Adleman number theoretic public key cryptosystem based on the encoding modulus m , i.e. a uniform lower bound on the number of residue classes modulo m which solve the congruence

$$x^c \equiv x \pmod{m};$$

3. A necessary and sufficient condition on c and m that the congruence

$$x^c \equiv x \pmod{m}$$

have no more than the number of solutions given by this aforementioned uniform lower bound, in other words that a Rivest-Shamir-Adleman key cryptosystem offer the maximum possible concealment.

In fact, 2 and 3 both follow from Theorem 3, which provides a formula for the number of unconcealable messages in a number theoretic public key cryptosystem of a general kind, which includes RSA cryptosystems as a special case. We need a few variants of standard notation for typographical simplicity. If T is a finite set of positive integers we let ΠT ($LCMT$, $GCDT$) be the product (least common multiple, greatest common divisor) of the members of T . Thus, for example,

$$\Pi\{x^2 | 1 \leq x \leq 4\} = \Pi\{1, 4, 9, 16\} = 576$$

$$LCM\{9, 12\} = 36$$

$$GCD\{9, 12, 15\} = 3.$$

As usual, void products are equal to 1.

We follow the terminology in [3, p. 1–80]. In what follows, T will denote a set of k odd primes, where $k \geq 2$, and the modulus m will be of the form

$$m = \Pi\{p^{a(p)} | p \in T\}$$

where the $a(p)$ are positive integers. The modulus m is square free [2, p. 16] if $a(p) = 1$ for all $p \in T$.

As usual ϕ is the Euler totient function [3, p. 27–31] and λ is the universal exponent function ([3], p. 53). Thus

$$\phi(m) = \Pi\{(p-1)p^{a(p)-1} | p \in T\}$$

$$\lambda(m) = LCM\{(p-1)p^{a(p)-1} | p \in T\}$$

since all the primes p are odd. For the modulus m used in the examples above

$$m = \Pi\{p | p \in T\} = 97 * 109 = 10573$$

$$\phi(m) = \Pi\{p-1 | p \in T\} = 96 * 108 = 10368$$

$$\lambda(m) = LCM\{p-1 | p \in T\} = 864.$$

Evidently we have $\phi(m) = 10368 = 12 * 864 = 12\lambda(m)$, in accordance with the observation[1] that $\lambda(m)$ is a factor of $\phi(m)$.

In the development below we will consider the following natural generalization of RSA cryptosystem.

Definition 1: A number theoretic public key cryptosystem is a list

$$(c, d, m)$$

of three integers, where m is square free and

$$2 \leq c \leq m - 1$$

$$2 \leq d \leq m - 1$$

$$cd \equiv 1 \pmod{\lambda(m)}.$$

Every public key cryptosystem of Rivest–Shamir–Adleman type[4] satisfies this definition. But the definition also covers other public key cryptosystems.

2. PERMUTING RESIDUE CLASSES BY TAKING POWERS

THEOREM 1. *Let $c \geq 2$ be an integer. Let $f(x) = x^c$. If m is not square free then f is not a permutation of the residue classes modulo m . If m is square free then f is a permutation of the residue classes modulo m if and only if c is relatively prime to $\lambda(m)$.*

Proof. If p^2 divides m then

$$(m/p)^c \equiv 0^c \pmod{m}$$

since $c \geq 2$. But $m/p \not\equiv 0 \pmod{m}$. This proves the first statement. Now let m be square free. The sufficiency of the condition

$$\text{GCD}\{c, \lambda(m)\} = 1$$

was proved for $k = 2$ in [4] and for $k \geq 2$ in [1]. Conversely suppose that

$$u = \text{GCD}\{c, \lambda(m)\} > 1.$$

Let g belong [3, p. 43] to the exponent $\lambda(m)$ modulo m and let

$$x(i) = g^{1+i\lambda(m)/u}$$

where $i = 0, 1, \dots, u - 1$. Clearly

$$x(i)^c \equiv g^c \pmod{m}$$

for all $i = 0, 1, \dots, u - 1$. On the other hand the congruence

$$x(i) \equiv x(j) \pmod{m}$$

would imply

$$i\lambda(m)/u \equiv j\lambda(m)/u \pmod{\lambda(m)},$$

whence

$$i \equiv j \pmod{u}.$$

Hence

$$i = j.$$

Thus there are u distinct elements mapped to the same element by f . This ends the proof.

COROLLARY 1. *If $f(x) = x^c$ is a permutation of the residue classes modulo m then m is square free and c is odd.*

3. UNCONCEALABLE MESSAGES ARE UNAVOIDABLE

THEOREM 2. *Let c and m be positive integers. Let c be odd. Then there are at least 3^k residue classes x modulo m such that*

$$x^c \equiv x \pmod{m}.$$

Proof. Recall that

$$m = \prod \{p^{a(p)} | p \in T\},$$

where T has k members. Clearly 0, 1 and -1 are solutions of the congruences

$$x^c \equiv x \pmod{p^{a(p)}}$$

for every $p \in T$. The result follows by combining these solutions, using the Chinese Remainder Theorem [3, p. 35].

In the RSA case $m = pq$, whence there are 9 messages which are unconcealable in any cryptosystem (c, d, m) . These 9 do not depend on the choice of c or d . Let us illustrate this by augmenting an example due to Rivest *et al.* ([4], p. 124) which has been augmented by Simmons and Norris[5, 6]. Let

$$\begin{aligned} p &= 47 \\ q &= 59 \\ m &= 2773. \end{aligned}$$

Then obviously

$$\begin{aligned} m &= 47 * 59 = pq \\ \phi(p) &= p - 1 = 46 \\ \phi(q) &= q - 1 = 58 \\ \phi(m) &= (p - 1)(q - 1) = 46 * 58 = 2668. \end{aligned}$$

If we note that

$$\begin{aligned} 2772 &= -1 + 59 * 47 = -1 + 47 * 59 \\ 2537 &= -1 + 54 * 47 = 0 + 43 * 59 \\ 2302 &= -1 + 49 * 47 = 1 + 39 * 59 \\ 235 &= 0 + 5 * 47 = -1 + 4 * 59 \\ 0 &= 0 + 0 * 47 = 0 + 0 * 59 \\ 2538 &= 0 + 54 * 47 = 1 + 43 * 59 \\ 471 &= 1 + 10 * 47 = -1 + 8 * 59 \\ 236 &= 1 + 5 * 47 = 0 + 4 * 59 \\ 1 &= 1 + 0 * 47 = 1 + 0 * 59 \end{aligned}$$

then we have found representatives of 9 residue classes modulo 2773 which are unconcealable

in any Rivest-Shamir-Adleman public key cryptosystem based on the encoding modulus $m = 2773$. Obviously if p and q are primes and $U(pq)$ is the set of residue classes which are unconcealable in any Rivest-Shamir-Adleman public key cryptosystem based on the encoding modulus pq , then $U(pq)$ contains the residue classes to which 0, 1 and $pq - 1$ belong. But 6 of the 9 members of $U(pq)$ depend strongly on p and q . It is shown in [1] that anybody who can find 1 of these latter 6 messages can thereby find p , and thus break the cryptosystem.

We will now derive a formula for the number N of residue classes x modulo m such that

$$x^c \equiv x \pmod{m}.$$

THEOREM 3.

$$N = \prod \{(1 + \text{GCD}\{c - 1, \phi(p^{a(p)})\}) | p \in T\}.$$

Proof. We prove the case $k = 1$ first. Thus we must show that the congruence

$$x^c \equiv x \pmod{p^a}$$

has $1 + \text{GCD}\{c - 1, \phi(p^a)\}$ solution classes modulo p^a . If, on the one hand, p is a factor of x and

$$x^c \equiv x \pmod{p^a}$$

then

$$x(x^{c-1} - 1) \equiv 0 \pmod{p^a}$$

but

$$x^{c-1} \not\equiv 1 \pmod{p}.$$

Therefore

$$x \equiv 0 \pmod{p^a}.$$

If, on the other hand, p is not a factor of x then

$$x = g^t,$$

where g is a primitive root [3, p. 49] modulo p^a . Thus

$$g^{tc} \equiv g^t \pmod{p^a}$$

if and only if

$$t(c - 1) \equiv 0 \pmod{\phi(p^a)}.$$

But this last congruence has $\text{GCD}\{c - 1, \phi(p^a)\}$ solutions. From the case $k = 1$, the general theorem can be derived by means of the Chinese Remainder Theorem.

COROLLARY 1. Let c be odd integer larger than 2. Then $N = 3^k$ if and only if $\text{GCD}\{c - 1, \lambda(m)\} = 2$.

Proof. Since $c - 1$ is even and $\phi(p^{a(p)})$ is even, then

$$\text{GCD}\{c - 1, \phi(p^{a(p)})\} \geq 2$$

for every $p \in T$. Therefore

$$N \geq \prod \{(1 + 2) | p \in T\} = 3^k.$$

Evidently equality holds if and only if

$$\text{GCD}\{c-1, \phi(p^{a(p)})\} = 2$$

for every $p \in T$. Therefore

$$\begin{aligned} \text{GCD}\{c-1, \lambda(m)\} &= \text{GCD}\{c-1, \text{LCM}\{\phi(p^{a(p)}) | p \in T\}\} \\ &= \text{LCM}\{\text{GCD}\{c-1, \phi(p^{a(p)})\} | p \in T\} \\ &= \text{LCM}\{2 | p \in T\} = 2. \end{aligned}$$

COROLLARY 2. *Let m be square free. Let c be an odd integer greater than 2. If there is an integer x such that*

$$x^c \not\equiv x \pmod{m},$$

then $5N \leq 3m$.

Proof. If $\lambda(m)$ were a factor of $c-1$ then the congruence

$$x^c \equiv x \pmod{m}$$

would be an identity in x because m is square free. Therefore $\lambda(m)$ is not a factor of $c-1$. So there is a prime $q \in T$ such that $q-1$ is not a factor of $c-1$. Hence

$$2 \leq \text{GCD}\{q-1, c-1\} \leq (q-1)/2,$$

from which it follows that

$$5 \leq q.$$

Also

$$1 + \text{GCD}\{q-1, c-1\} \leq (q+1)/2.$$

If $p \in T \setminus \{q\}$ then

$$1 + \text{GCD}\{c-1, p-1\} \leq p.$$

Therefore

$$\begin{aligned} N/m &\leq (1+q)/2q \\ &= 1/2 + 1/2q \\ &\leq 1/2 + 1/10. \end{aligned}$$

It is clear from the proof that equality holds if and only if m is a square free multiple of 5, and $c-1$ is a multiple of $\lambda(m/5)$.

4. PERMUTING EXPONENTS, DERANGING EXPONENTS AND OPACITY.

It is worthwhile to have a brief explicit way of verifying that a proposed encoding scheme actually effects a permutation of the messages. To recap our results along these lines we state a definition and a theorem.

Definition 2. Let m be a square free odd positive integer. Let c be a positive integer. Then c is called a permuting exponent for m if every pair x, y of integers which satisfies the congruence

$$x^c \equiv y^c \pmod{m}$$

also satisfies the congruence

$$x \equiv y \pmod{m}.$$

We have already proved that c is a permuting exponent for m if and only if c is relatively prime to $\lambda(m)$.

As we have seen, the question of concealment is a complex one. An encoding exponent can effect a permutation of the residue classes modulo m , but no exponent can effect a derangement of these residue classes. At least 9 residue classes must be unchanged. More residue classes may be. There should, however, be a name and a criterion for encoding exponents which come as close as possible to effecting a derangement of the residue classes modulo m . Hence another definition and theorem.

Definition 3. Let m be a square free odd positive integer. Let c be a permuting exponent for m . Then c is called a deranging exponent for m if every integer x which satisfies the congruence

$$x^c \equiv x \pmod{m}$$

also satisfies the congruence

$$x^3 \equiv x \pmod{m}.$$

The foregoing discussion has proved that c is a deranging exponent for m if and only if

$$\begin{aligned} \text{GCD}\{c, \lambda(m)\} &= 1 \\ \text{GCD}\{c-1, \lambda(m)\} &= 2. \end{aligned}$$

The criterion above is not very stringent. In the RSA case we see that c is a deranging exponent for m if and only if

$$\begin{aligned} \text{GCD}\{c, (p-1)(q-1)\} &= 1 \\ \text{GCD}\{c-1, \text{LCM}\{p-1, q-1\}\} &= 2. \end{aligned}$$

Note that $\lambda(m)$ can be replaced by $\phi(m)$ in the first equation, but not the second.

THEOREM 4. Let m be square free. Then the number of deranging exponents c for m , which lie in the range $0 < c < \lambda(m)$, is

$$(\lambda(m)/f) \prod \{1 - 2/q \mid q \text{ is an odd prime factor of } \lambda(m)\}$$

where $f = 4$ if 4 is a factor of $\lambda(m)$, and $f = 2$ if 4 does not divide $\lambda(m)$.

Comment. The proof below is a constructive one. It can be used to find the deranging exponents in question.

Proof. Let W be the set of odd prime factors of $\lambda(m)$. We can write the prime factorization of $\lambda(m)$ as

$$\lambda(m) = 2^{v(2)} \prod \{q^{v(q)} \mid q \in W\}.$$

The first case to consider is $v(2) = 1$. Here we have $\text{GCD}\{c, \lambda(m)\} = 1$ if and only if

$$\text{GCD}\{c, 2\} = 1$$

and

$$\text{GCD}\{c, q^{v(q)}\} = 1$$

for every $q \in W$. This means that

$$c \not\equiv 0 \pmod{2}$$

and that

$$c \not\equiv hq \pmod{q^{v(q)}}$$

for $h \in Y(q) = \{1, 2, \dots, q^{v(q)-1}\}$. Also

$$\text{GCD}\{c - 1, \lambda(m)\} = 2$$

if and only if

$$\text{GCD}\{c - 1, q^{v(q)}\} = 1$$

for every $q \in W$ or, equivalently

$$c \not\equiv 1 + hq \pmod{q^{v(q)}}$$

for $h \in Y(q)$. Evidently the set $1 + Y(q)$ is disjoint from $Y(q)$. The number of residue classes modulo $q^{v(q)}$ which do not belong to

$$Y(q) \cup (1 + Y(q))$$

is $q^{v(q)} - 2q^{v(q)-1}$, which is positive since $q \geq 3$ for every $q \in W$. Using the Chinese Remainder Theorem we can now construct all the deranging exponents for m . There are

$$1 * \Pi\{q^{v(q)} - 2q^{v(q)-1} | q \in W\} = (\lambda(m)/2)\Pi\{1 - 2/q | q \in W\}$$

of them. In the second case $2 \leq v(2)$. This time the simultaneous equalities

$$\begin{aligned} \text{GCD}\{c, \lambda(m)\} &= 1 \\ \text{GCD}\{c - 1, \lambda(m)\} &= 2 \end{aligned}$$

are equivalent to the statements

$$\text{GCD}\{c, 2^{v(2)}\} = 1 \tag{1}$$

$$\text{GCD}\{c - 1, 2^{v(2)}\} = 2 \tag{2}$$

$$\text{GCD}\{c, q^{v(q)}\} = 1 \tag{3}$$

$$\text{GCD}\{c - 1, q^{v(q)}\} = 1 \tag{4}$$

for every $q \in W$. Conditions (3) and (4) are treated exactly as in the first case above, and again provide

$$q^{v(q)} - 2q^{v(q)-1}$$

residue classes modulo $q^{v(q)}$ to which c can belong. Conditions (1) and (2) are equivalent to the congruence

$$c \equiv 3 \pmod{4},$$

which provides $2^{v(2)-2}$ residue classes modulo $2^{v(2)}$ to which c can belong. Here, too, the Chinese Remainder Theorem can be used to construct all deranging exponents for m . This time there are

$$(\lambda(m)/4)\Pi\{1 - 2/q | q \in W\}$$

of them. The arguments above remain valid when W is void and, consequently, the products are equal to 1. This ends the proof.

A deranging exponent c in a number theoretic public key cryptosystem based on m cannot provide concealment of 100% of all possible messages which can be sent in that system, but it nevertheless provides as much concealment as possible. So we need a measure of the ability of a cryptosystem to conceal messages.

Definition 4. Let a number theoretic public key cryptosystem have encoding modulus m and encoding exponent c . Let N be the number of residue classes modulo m whose members satisfy the congruence.

$$x^c \equiv x \pmod{m}.$$

Then the *opacity* of the cryptosystem is

$$1 - N/m,$$

whether expressed as a real number or as a per cent.

Theorem 2 showed that no number theoretic public key cryptosystem can have 100% opacity. Corollary 2 showed that no cryptosystem can have an opacity strictly between 0% and 40%. In the RSA case the two prime factors of m exceed 10^{50} , and a look at the proof of Corollary 2 shows that opacity must exceed 49.99999% if it is nonzero.

REFERENCES

1. Bob Blakley and G. R. Blakley, Security of number theoretic public key cryptosystems against random attack, I, II, III. *Cryptologia* 2(4), 305-321 (1978), 3(1), 29-42 (1979), 3(2), 105-118 (1979).
2. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th Edn. Oxford University Press, London (1965).
3. W. J. Leveque, *Topics in Number Theory*. Vol. 1, 1st Edn. Addison-Wesley, Reading, Massachusetts (1958).
4. R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems. *Communs ACM* 21(2), 120-126 (1978).
5. R. L. Rivest, Remarks on a proposed cryptanalytic attack of the M.I.T. public key cryptosystem. *Cryptologia* 2(1), 62-65 (1978).
6. G. J. Simmons and J. N. Norris, Preliminary comments on the M.I.T. public key cryptosystem. *Cryptologia* 1(4), 406-414 (1977).